Wireless Local Area Networks

Uwe Hübner

Technische Universität Chemnitz
huebner@hrz.tu-chemnitz.de

Wireless Local Area Networks (WLAN) findet man zunehmend als Trägersystem für die mobile Kommunikation mit Notebooks und Handhelds im Campusbereich und darüber hinaus.
In diesem Tutorium werden die typischen Einsatzszenarien von WLANs vorgestellt, wobei auch ein Blick auf verwandte Technologien und Alternativen nicht fehlt.
Die WLAN-Funktionsprinzipien werden an Hand der verbreiteten Standards IEEE 802.11, 802.11b und 802.11a erläutert. Hieraus ergeben sich die wesentlichen Eigenschaften im Hinblick auf die Nutzung des Frequenzspektrums und die zu erwartenden Datenraten. Durch eine zweckmäßige Auswahl der Betriebsmodi kann unterschiedlichen Einsatzzwecken Rechnung getragen werden.
Die bei drahtlosen Netzen naturgemäß etwas schwierigere Situation zur Netzsicherheit wird transparent gemacht. Die Möglichkeiten und Grenzen der einsetzbaren Verfahren werden erklärt, um die Auswahl adäquater Techniken und Vorkehrungen für den jeweiligen Anwendungsfall zu unterstützen.
Für die konkrete Planung einer WLAN-Infrastruktur wird das erforderliche Überblickswissen zur Funkausbreitung vermittelt. Eine kurze Kommentierung des gegenwärtig verfügbaren Produktspektrums und ein Ausblick runden das Tutorium ab.

1 Einführung

1.1 Einsatzgebiete von WLANs

LANs in Ethernet-Technik haben mittlerweile einen hohen Reifegrad bei verhältnismäßig niedrigen Kosten erreicht. Wenn hier Alternativen und/oder Ergänzungen behandelt werden, stellt sich natürlich die Frage nach der Notwendigkeit und Sinnfälligkeit. Eine neue Technik sollte nicht (nur) deswegen eingesetzt werden, weil sie gerade verfügbar und „in Mode“ ist. Die Begründung sollte vielmehr aus den Anwendungsfällen heraus gegeben sein.

Eine sehr kurze Antwort läßt sich mit diesem Ausdruck geben:

any∗
anywhere, anytime, anything ... :-)

Wir wollen nahezu beliebige Kommunikationsdienste jederzeit unabhängig von unserem augenblicklichen Aufenthaltsort nutzen.
Wenn wir die Anwendungsfälle etwas differenzierter betrachten, können wir einige **Szenarien** unterscheiden:

- Mitarbeiter wollen/müssen Laptops an wechselnden Orten einsetzen
- Kontakt zu mobilen Mitarbeitern und mobiler Technik
- Mobile Nutzer untereinander
- Bei schwierigen Verkabelungsverhältnissen
- Kurzzeitige Nutzungsfälle
- Backup für Festnetz
- Variable Zahl von temporären Zugängen
- Öffentliche „Hot-Spots“
- *Community Networks*

Im Hochschulbereich erlebt die WLAN-Technik eine recht zügige Verbreitung. Hier lassen sich eine Reihe spezifischer Anwendungsgebiete nennen:

- Zugriff auf Multimedia-Material
- Interaktion in Übungen und Seminaren
- Selbststudium und Studienorganisation
- Tagungen, Ausstellungen ...
- ... als Lehrgegenstand

Einen wesentlichen Anstoß hat die in den Jahren 2000/2001 realisierte BMBF-Initiative zur Förderung von Demonstrationsprojekten für die Funkvernetzung (WLAN) von Hochschulen gegeben:

http://wlan.informatik.uni-rostock.de/hochschulen/

1.2 Alternativen

Die WLAN-Technik steht nicht isoliert da, es gibt eine Reihe weiterer drahtloser Techniken, die ähnliche Ziele und Eigenschaften haben.
Hier wollen wir die wichtigsten benachbarten Techniken anführen. Aus den Unterschieden bei den technischen Eigenschaften ergeben sich Abgrenzungen der Einsatzdomänen. Wir werden aber auch Überlappungen finden, die eine Einsatzentscheidung schwieriger machen. Für die Aussichten einer Technologie sind nicht nur rein technische Parameter maßgebend, mindestens ebensoviel Einfluß haben Verbreitung, wirtschaftliche und regulatorische Einflüsse.

- **Infrarot**
  Infrared Data Association (IrDA)
  115 kbit/s ... 4 Mbit/s
  Reichweite mindestens 1 m (typ. 2m)
  http://www.irda.org
- **Bluetooth**, IEEE **802.15**
  Wireless Personal Area Network (WPAN)
  .. 1 Mbit/s,
  2,4 GHz-ISM-Band, Übertragungsverfahren FHSS
  Reichweite mindestens 1 m (... 10m)
  Sendeleistung ca. 1 mW (.. energiesparendes Design)

http://www.bluetooth.com/

– **HomeRF**: „Consumer"-WLAN,
als Nachfolger von **Digital European Cordless Telecommunications (DECT)** positioniert,
1,6 Mbit/s (.. 10 Mbit/s)
http://www.homerf.org/

– **Mobilfunknetze der 3./4. Generation**
Das als Mobilfunknetz der 3. Generation bezeichnete **Universal Mobile Telecommunications System (UMTS)** liefert Bandbreiten, die mehr als eine Größenordnung unter denen von WLANs liegen. Auch die Situation bei den laufenden Kosten dürfte sich deutlich anders als bei WLAN darstellen.
Erste Überlegungen zu Mobilfunknetzen der 4. Generation wurden publiziert. Es ist nicht unwahrscheinlich, daß diese Generation der WLAN-Technik näher ist als der Tradition der Mobiltelefonie.
Der relative Anteil der Sprachkommunikation wird zwar zurückgehen, ein wesentliches Element wird sie aber bleiben. Im Gefolge der Verbreitung von **Voice over IP (VoIP)** ist *„Voice-over-IP-over-WLAN"* durchaus realistisch.

Eine Koexistenz der Techniken für sehr unterschiedliche Versorgungsbereiche ist wahrscheinlich:

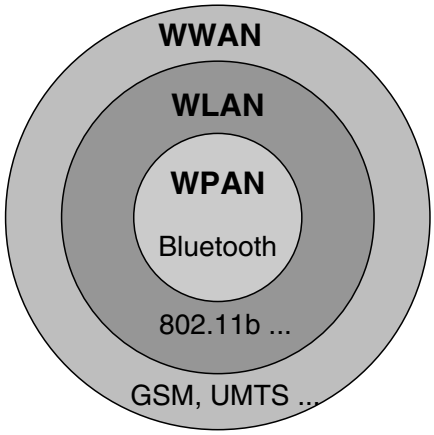

Abbildung 1: Koexistenz der drahtlosen Netze

2 Funktionsweise und Technik von WLANs

2.1 IEEE 802.11/802.11b

Erste drahtlose lokale Netze gab es seit etwa 1992. Bei den frühen Produkten mußte man sich mit Bandbreiten deutlich unter 1 Mbit/s begnügen. Noch unangenehmer war die feh-

lende Standardisierung, nur Produkte eines Typs von einem (vielleicht kurzlebigen) Hersteller waren untereinander interoperabel.
Diese Situation verbesserte sich entscheidend mit der Verabschiedung des 802.11-Standards, der danach noch verschiedene Erweiterungen erfahren hat:

- 1997: IEEE **802.11** - 1/2 Mbit/s
- 1999: IEEE **802.11b** - 11 Mbit/s

Frequenzbereich:

- 2.4 - 2.4835 GHz
- **Industrial, Scientific, and Medical (ISM)**
- lizenzfreie Nutzung mit niedrigen Leistungen
- max 100 mW, praktisch 10 .. 30 mW

Übertragungsverfahren bei 802.11:

- **Frequency Hopping Spread Spectrum (FHSS)**
- **Direct Sequence Spread Spectrum (DSSS)**
  bei 802.11b wird nur noch DSSS verwendet

Die Spreizspektrum-Techniken (*Spread Spectrum*) wurden ursprünglich für militärischen Funkverkehr entwickelt. Durch die Aufspreizung des Signals auf ein breites Frequenzspektrum ist dieses Signal von unerwünschten Mithörern schwieriger festzustellen als ein herkömmliches schmalbandiges Funksignal.

> *Dies gilt allerdings strenggenommen nur, wenn der Mithörer die exakten Parameter des Signals nicht kennt.*

Daneben ist dieses Signal auch durch schmalbandige Funksignale nur schwer zu stören. Selbst andere Spreizspektrum-Signale wirken nur wenig störend, wenn sich die Spreizvorschriften unterscheiden.
Da bei WLANs mittlerweile DSSS-Verfahren die Hauptrolle spielen, werden wir uns diese nachfolgend näher ansehen.

Oft werden mehrere WLANs bzw. mehrere Zellen eines WLAN mit überlappenden Funkbereichen betrieben. Hier ist es vorteilhaft, unterschiedliche Frequenzbereiche zu benutzen, um die gegenseitigen Beeinflussungen zu minimieren. Eine Separierung auf der logischen Ebene („Netzname“) ist zwar auch möglich, allerdings ohne eine Vervielfachung der Bandbreite.

Die **Kanalaufteilung** für DSSS hat folgende Merkmale:

- Kanalbreite je 22 MHz, überlappend!
- in Deutschland 13 Kanäle (ETSI), U.S., Kanada: 11

Es existieren also nur drei **nichtüberlappende** Kanäle. Im Idealfall wird man z.B. nur die Kanäle 1, 6 und 11 vergeben:

Praktische Funkzellen sind natürlich (leider) nicht wabenförmig, auch halten sich die Funkwellen nicht an eine exakte Grenze.

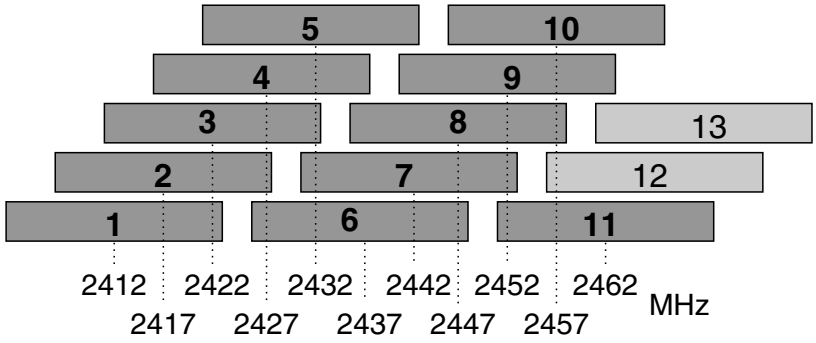

Abbildung 2: Kanalaufteilung 2,4 GHz

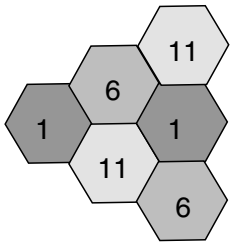

Abbildung 3: Kanalvergabe-Beispiel

Mit nur drei nichtüberlappenden Kanälen wird man typischerweise keine Versorgung einer Fläche ohne Interferenzen erzielen. Die Nutzung von Kanälen mit Überlappung ist dann oft ein brauchbarer Kompromiß, denn der Störeinfluß nimmt durch den Kanalversatz doch etwas ab.

> Ein wesentlicher Zusammenhang besteht zwischen der **Zellengröße** und der **Bandbreite pro Fläche**. Letztere können wir erhöhen, wenn wir **kleinere** Zellen bilden. Das funktioniert aber nur, wenn wir gleichzeitig die Reichweiten, d.h. die Sendleistungen verringern!

Beim Übertragungsverfahren **Direct Sequence Spread Spectrum** nach 802.11 wird die Nutzinformation mit einem Spreizkode XOR-verknüpft:

Mit einem **Modulationsverfahren** wird nun dieses Resultat einem Träger aufmoduliert, wobei zwei oder vier Phasen verwendet werden. Das ergibt dann ein bzw. zwei kodierbare Bits pro Schritt. Mehr Zustände bedeuten eine höhrere Datenrate, allerdings auch einen größeren Signal/Störabstand und damit geringere Reichweite.

- 1 Mbit/s: **Differential Binary Phase Shift Keying (DBPSK)**
- 2 Mbit/s: **Differential Quadrature Phase Shift Keying (DQPSK)**
- 11/5,5 Mbit/s (802.11b): **Complementary Code Keying (CCK)** + DQPSK
  Um die höheren Datenraten zu erreichen, wird bei 802.11b kein konstanter Spreizkode mehr verwendet, sondern dieser als zusätzliches Kodierelement genutzt.

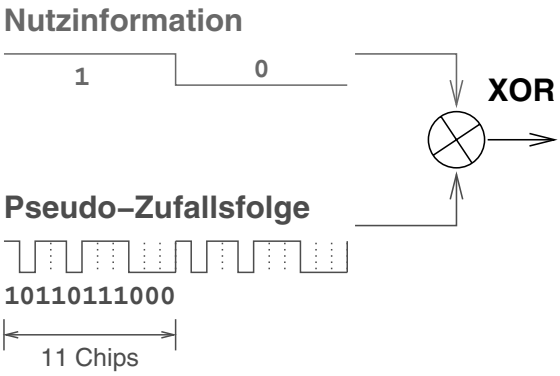

Abbildung 4: DSSS für 1/2 Mbit/s

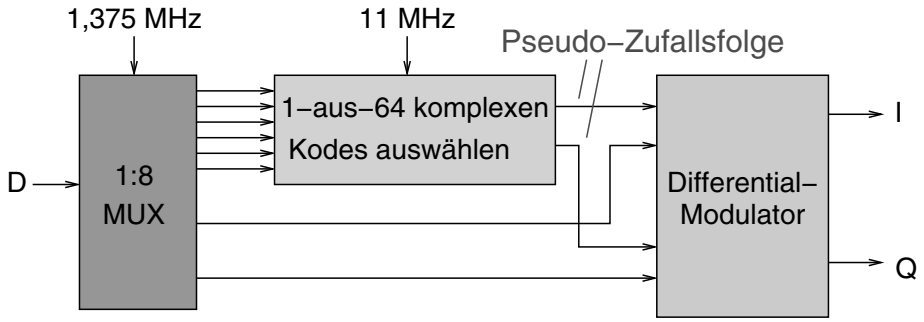

Abbildung 5: CCK-Erzeugung

Statt 11-Bit-Barker-Kode wird ein komplexer 8-Bit-Kode verwendet, aus den möglichen 4^8 Kodeworten werden 64 mit möglichst optimaler Distanz ausgewählt.
Die Symbolrate ist 1,375 Msym/s

2.2 IEEE 802.11a

Im praktischen Einsatz dominieren heute WLANs nach 802.11b, wobei die Entwicklung aber hier nicht stehenbleiben wird. Die Suche nach neuen technischen Lösungen wurde einmal durch den Bedarf an höheren Datenraten motiviert. Weiterhin ist das bei 802.11b genutzte 2,4-GHz-ISM-Frequenzband relativ schmal. Wegen der zahlreichen weiteren Nutzungen (z.B. *Bluetooth*) sind gegenseitige Beeinträchtigungen zu erwarten. Im Bereich um 5 GHz gibt es ein weiteres Band, welches für WLAN in Frage kommt, dies ist die Domäne des Standards 802.11a.

– Datenrate **6**, 9, **12**, 18, **24**, 36, 48, **54** Mbit/s

– 5 GHz
  U.S.: **Unlicensed National Information Infrastructure (U-NII)**

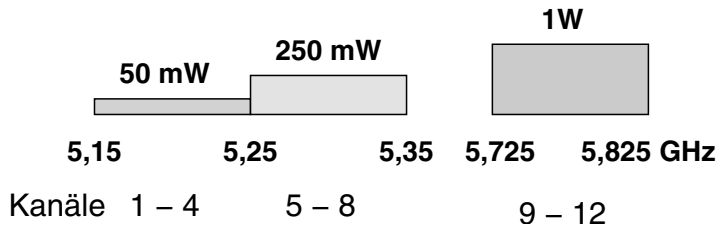

Abbildung 6: Kanalaufteilung (U.S.)

In Europa besteht bislang eine Frequenzzuweisung 5,15-5,35 + 5,47-5,725 für HIPERLAN/2

– 12 nicht-überlappende Kanäle
– **Orthogonal Frequency Division Multiplexing (OFDM)**
  ist das hier verwendete neue Übertragungsverfahren. Es bedient sich einer größeren Anzahl von Unterträgern (*Subcarrier*), die jeweils Teildatenströme übertragen.

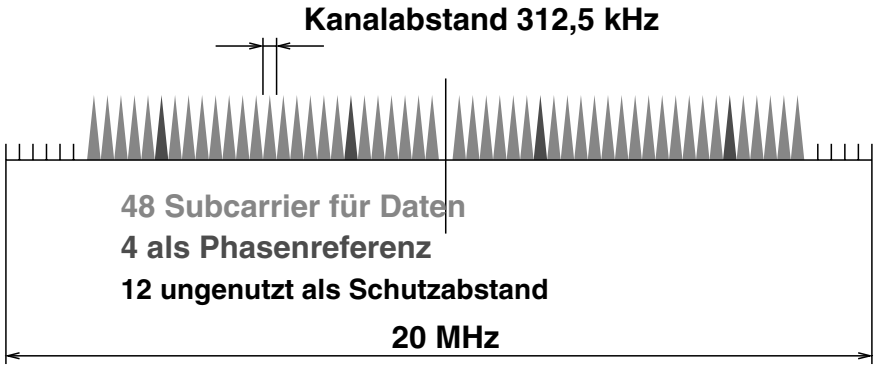

Abbildung 7: Subcarrier-Aufteilung

Je Subcarrier wird eine 64-QAM verwendet, für niedrigere Raten (geringerer Signal/Störabstand) auch 16-QAM, QPSK, BPSK.

– **Forward Error Correction (FEC)** wird eingesetzt.
– Durch die höheren Frequenzen sind eigentlich etwas geringere Reichweiten als bei 802.11b zu erwarten, vor allem bei Hindernissen mit höherem Absorbtionsvermögen (massive Wände ...).
  Eine Messung aus

http://www.atheros.com/AtherosRangeCapacityPaper.pdf
zeigt aber, daß unter günstigen Bedingungen die Datenrate von 802.11a bei jeder Entfernung oberhalb der von 802.11b bleibt.

Es ist damit zu rechnen, daß in Kürze 802.11a auch in Europa zugelassen ist. Dieser Standard wird hinsichtlich Produktverfügbarkeit und Kosten gut mit 802.11b konkurrieren können. Aus diesem Grund wollen wir uns die Entscheidungskriterien für 802.11a im Vergleich mit 802.11b ansehen:

+ Notwendigkeit hoher Datenraten
+ keine Interferenz mit anderen Nutzern von 2,4 GHz
+ hohe Nutzerdichte
- Reichweite bei Hindernissen geringer
- eventuelle Migrationskosten von 802.11b nach 802.11a
- geringere Nutzerdichte, größere Reichweiten erwünscht

Die Entscheidung wird möglicherweise kein entweder-oder sein müssen, denn es gibt Koexistenz-Varianten:

– *Dual-Standard*-APs
– *Dual-Standard*-Chipsets

Mit 802.11a ist noch nicht das Ende der Entwicklung erreicht, vielmehr gibt es eine ganze Reihe weiterer Richtungen, die hier nur kurz genannt werden sollen:

– **HIPERLAN/2**: bis 54 Mbit/s, 5,15-5,35 GHz
Higher Performance Radio LAN (HIPERLAN), ETSI
– **802.11g**: 22 ... 54 Mbit/s, 2,4 GHz, 30-50m
– **802.11e**: MAC Enhancements (QoS ...)
– **802.11f**: Inter-Access Point Protocols
– **802.11i**: Security Enhancements
– **802.16**: Wireless MAN, fixed **Broadband Wireless Access (BWA)**, 2 ... 66 GHz,

2.3 Kanalzugriff und Rahmenstruktur

Das Medium „Funk“ ist in gewisser Hinsicht mit dem traditionellen Ethernet vergleichbar, bei dem mehrere Stationen um den Zugriff auf ein Medium (bzw. jetzt ein Frequenzband) konkurrieren. Bei WLANs nach 802.11 werden folgende Verfahren zur Koordinierung des Medienzugriffs eingesetzt:

– **Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA)**
Eine sendewillige Station prüft, ob das Medium (der Funkkanal) frei ist. Das vom Ethernet bekannte CSMA/CD ist nicht einsetzbar, weil eine Station während des Sendens kaum feststellen kann, ob eine weitere Station ebenfalls sendet.
– **Distributed Coordination Function (DCF)**
Eine absolute Vermeidung von Kollisionen ist nicht gegeben. Allerdings wird die Zeitspanne, in der Kollisionen vorkommen können, durch ein geschicktes Verfahren minimiert:

1. Station wartet Pause mit einer Mindestlänge ab
   DCF Inter-Frame Spacing (DIFS)
2. Empfänger quittiert nach kurzer Pause
   Short Inter-Frame Spacing (SIFS)
3. bei „besetzt“: DIFS + Zufallswert (**Backoff**) abwarten
   „Fairness“: Zufallswert wird nach eigenem Senden gesetzt, sonst heruntergezählt

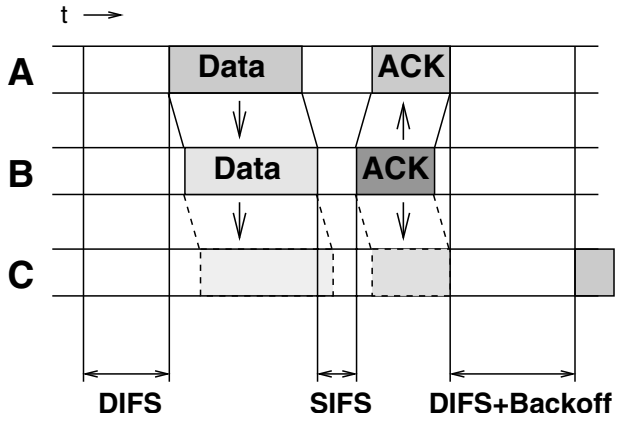

Abbildung 8: Kanalzugriff

– Wegen der endlichen Ausbreitungsgeschwindigkeit kann es natürlich trotzdem zu Kollisionen kommen, wenn zwei Stationen nahezu zum selben Zeitpunkt einen freien Kanal feststellen und zu senden beginnen. Durch die ausbleibende Quittung (ACK) kann die Kollision erkannt werden. Eine Zufallskomponente bei der Zeit bis zum Wiederholversuch sorgt dafür, daß die beiden Stationen beim nächsten Mal (höchstwahrscheinlich) nicht wieder kollidieren.
  Der eben beschriebene Mechanismus funktioniert allerdings nur dann korrekt, wenn alle Stationen alle anderen auch empfangen können (in unserem Beispiel kann C sowohl A als auch B empfangen). Mitunter wird das nicht gegeben sein, wenn zwischen bestimmten Stationen Hindernisse vorhanden sind. Wir bezeichnen dies als das Problem der ***hidden nodes***. Eine Station D, die A nicht empfangen kann, könnte beispielsweise mitten während der Daten-Sendung von A beginnen.
  Für diesen Fall gibt es den (optionalen) Mechanismus **Request to send/Clear to send (RTS/CTS)**.
  Den erreichten Effekt bezeichnet man als **Virtual Carrier Sense**.
  *RTS- und CTS-Rahmen enthalten eine Längenangabe für **Data**.*
– Optional ist eine **Point Coordination Function (PCF)**, bei der die Zugriffskoordinierung durch den *Access Point* erfolgt.
  Damit lassen sich beispielsweise definierte Teilbandbreiten vergeben (Stichwort „Multimedia“ ...)

Hier sehen Sie die Rahmenstruktur des **Physical Layer Convergence Protocol (PLCP)**:

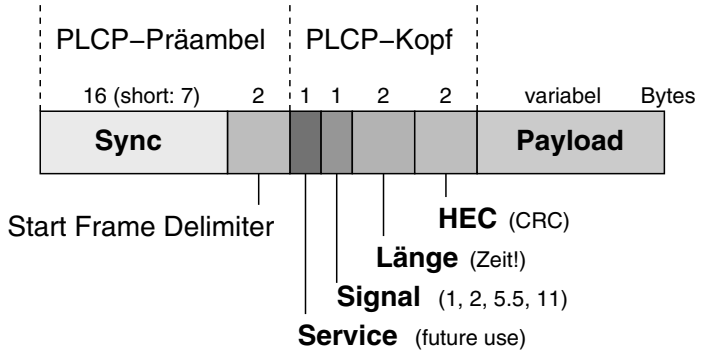

Abbildung 9: PLCP bei 802.11/11b

In der *Payload* haben wir dann folgende Rahmenstruktur:

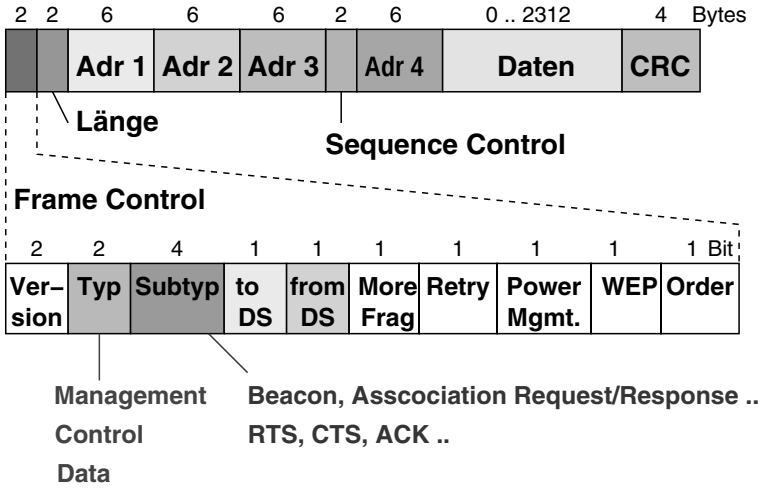

Abbildung 10: MAC-Rahmen bei 802.11

Die bis zu vier vorhandenen MAC-Adressen haben folgende Semantik:

toDS/fromDS	Adr 1	Adr 2	Adr 3	Adr 4
00 innerhalb Zelle	Ziel	Quelle	AP	
01 von außerhalb	Ziel	AP	Quelle	
10 nach außerhalb	AP	Quelle	Ziel	
11 zu anderer Zelle	Ziel-AP	AP	Ziel	Quelle

DS - Distribution System

2.4 Betriebsmodi

Eine wichtige Unterscheidung sind die unterschiedlichen **Betriebsmodi** eines WLAN:

- **Independent Basic Service Set (IBSS)**,
  Ad-Hoc, **Peer-to-Peer (P2P)**
  - für **Mobilstationen (MS)** untereinander

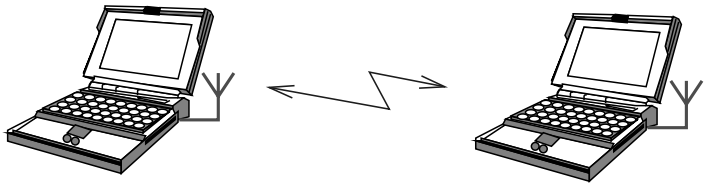

Abbildung 11: Ad-Hoc-Modus

- **Basic Service Set (BSS)**,
  Infrastruktur,
  managed
  - mit **Access Point (AP)**
- **Extended Service Set (ESS)**
  - Subnetz mit mehr als einem AP

  Als neue Anforderung kommt hier die Übergabe einer mobilen Station zwischen den APs hinzu, das sogenannte **Roaming**.
- **Point-to-Point** als Spezialfall

Für die **Kontaktaufnahme** einer Mobilstation mit einem AP gibt es zwei Alternativen:

- AP sendet periodisch „Bakeninformation“ (*Beacon*)
- Mobilstation sendet *Probe Request*,
  AP antwortet mit *Probe Response*

Ein AP kann unterschiedliche Funktionalitäten hinsichtlich der Behandlung von MAC-Rahmen oder darin eingepackten IP-Paketen realisieren. Wir unterscheiden diese Funktionalitäten für APs:

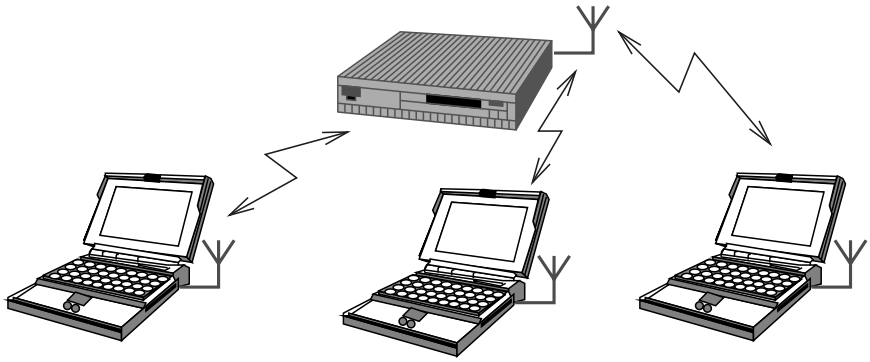

Abbildung 12: Infrastruktur-Modus

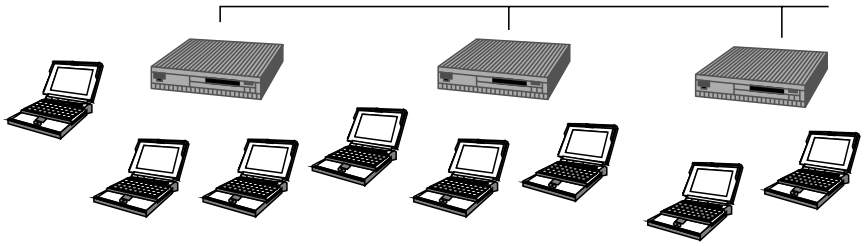

Abbildung 13: Infrastruktur-Modus mit mehreren APs

- **L2-Bridging**
  Das ist die heute gebräuchlichste Funktionalität. Wie bei einer Bridge (bzw. einem L2-Switch) „lernt“ der AP, welche MAC-Adressen wo angeschlossen sind. Alle APs befinden sich in einem IP-Subnetz.
- **Routing**
  WLAN- und Festnetzanschluß bilden unterschiedliche Subnetze. Die Routingregeln müssen von Hand oder durch entsprechende Routing-Protokolle eingestellt werden.
- **Network Address Translation (NAT)**
  Das ist eine Modifikation der Routing-Variante, bei der zusätzlich Quell- und/oder Zieladressen in den IP-Paketen modifiziert werden.
  Für das WLAN-Subnetz braucht man nun keine weltweit eindeutigen IP-Adressen mehr, sondern kann z.B. Adressen aus dem Bereich für „private Internets“ vergeben (192.168.0.0 .. 192.168.255.255 ...).

Zum Thema **Roaming** gibt es sehr unterschiedliche Ansätze:

- Die APs verständigen sich untereinander über bevorstehende Übergaben (die Mobilstation wird bei einem AP schwächer, bei einem anderen stärker). Mit heute eingesetzten Produkten müssen sich dazu alle APs in demselben Subnetz befinden (L2-Bridging). Die eingesetzten Protokolle sind meist herstellerspezifisch, nur bei (glei-

chen) APs eines Herstellers kann man von der Verfügbarkeit dieser Funktionalität ausgehen.

– Einen anderen Lösungsansatz bietet **Mobile IP**, potentiell auch mit APs in unterschiedlichen Netzen. Wegen der notwendigen Infrastruktur (Klientenkode, Home-Agents ...) und teilweise offener Fragen (Authentifizierung) ist die Nutzung von Mobile IP allerdings wenig verbreitet.
– Recht aussichtsreich sieht die Lösung des Problems auf der Anwendungsebene aus. Eine Reihe sehr verbreiteter Anwendungen der Peer-to-Peer-Techniken kann eine Konnektivität für Anwendungen auch bei wechselnden IP-Adressen aufrechterhalten. *Instant Messaging*-Produkte enthalten üblicherweise ein Präsenz-Management, das auch mit wechselnden IP-Adressen einer Mobilstation umgehen kann.

3 Sicherheitsaspekte bei WLANs

3.1 Elemente der Sicherheit

Wir haben eine neue Situation gegenüber Ethernet, die nicht immer richtig verstanden und behandelt wird, was diese (zu) pauschalen Aussagen illustrieren:

> *„Durch die verwendete Spreizbandtechnik (FHSS oder DSSS) ist ein Abhören nur mit sehr großem Aufwand möglich“*
> *„Die Wahl einer geheimen Netzwerk-ID grenzt die potenziellen Mithörer auf den Kreis ein, dem diese ID bekannt ist.“*
> *„Access-Control-Table-Mechanismen (an einen User gebundene Zugriffsrechte) stellen eine weitere Sicherheitsfunktion dar“*

Mit welchen Problemen müssen wir rechnen?

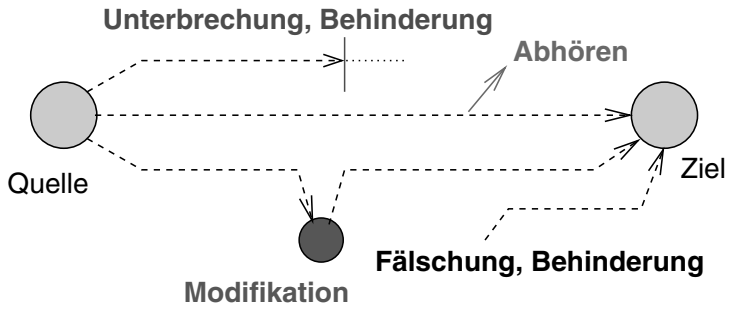

Abbildung 14: Gefährdungen

Wir sehen hier dieselben Gefährdungsklassen, die wir schon von drahtgebundenen Netzen kennen. Wie dort ist Sicherheit auch relativ und muß immer eine angemessene Wertigkeit

gegenüber den oft konkurrierenden Merkmalen wie Nutzerfreundlichkeit oder Performanz erhalten.

Bei den Vorkehrungen zur WLAN-Sicherheit werden wir diese Teilaspekte unterscheiden:

- Authentifizierung und Autorisierung
- Integrität
- Vertraulichkeit

Vorkehrungen zur Sicherheit können in ganz verschiedenen Schichten angeordnet werden. Damit wird klar, daß hier keineswegs nur WLAN-spezifische Techniken eine Rolle spielen. Einige der Techniken sind alternativ, aber auch Kombinationen sind oft sinnvoll.

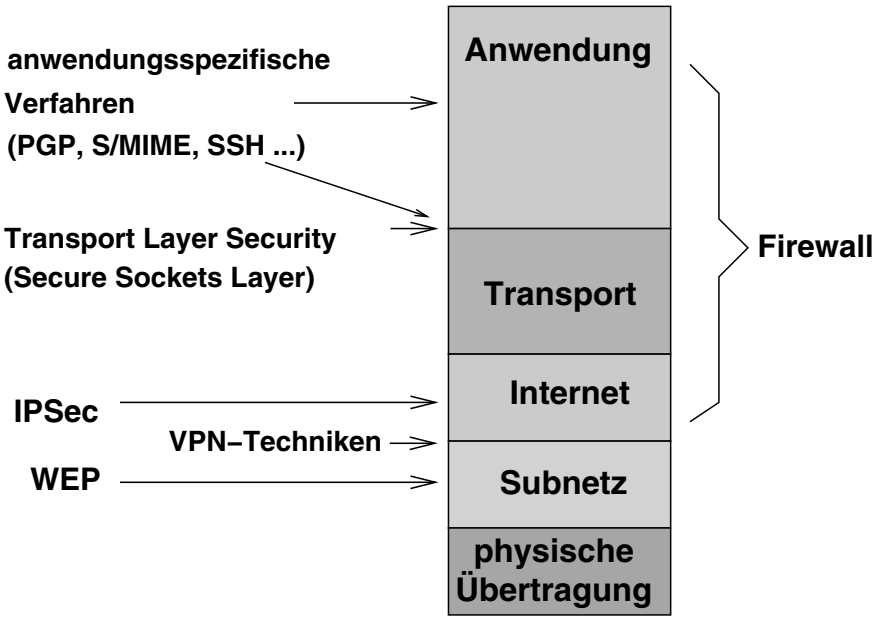

Abbildung 15: Einordnung der verschiedenen Techniken

Netzsicherheit hat auch eine nichttechnische Seite. Viele Probleme haben ihre Ursache „vor dem Bildschirm“. Eine Qualifizierung und Sensibilisierung der Nutzer wird insbesondere dann dringend erforderlich sein, wenn die Nutzer ihre Systeme selbst „managen“, was heute vielfach die Regel ist.
Ein Beispiel für einen Qualifikationsnachweis zur Nutzung privater Laptops an einer WLAN-Infrastruktur finden Sie hier:

http://www.tu-chemnitz.de/urz/ZIN/

EMVU

Zum Gebiet Sicherheit in einer etwas anderen Bedeutung gehören die potentiellen Auswirkungen elektromagnetischer Strahlung auf Organismen. Dies drückt sich im Begriff **Elektromagnetische Verträglichkeit Umwelt (EMVU)** aus. Gegenwärtig wird im Zusammenhang mit dem Ausbau der Mobilfunknetze der 2. und 3. Generation heftig um Grenzwerte, Genehmigungsverfahren usw. diskutiert.
WLANs sind hier allerdings weniger betroffen als beispielsweise GSM-Mobiltelefone, die eine etwa 50-fache Leistung abgeben. Trotzdem ist es sicherlich angeraten, durch Messungen die Einhaltung von Grenzwerten zu verifizieren und neue Erkenntnisse auf diesem Gebiet zu verfolgen.

Report - Mobile Phones and Health
[http://www.iegmp.org.uk/IEGMPtxt.htm]
Independent Expert Group on Mobile Phones

D. Tavangarian u.a.: Ergebnisse der Untersuchung der Einsatzmöglichkeiten von Notebooks in Lehre und Ausbildung an Hochschulen. S. 87-96
[http://www.gmd.de/PT-NMB/Bereich_Hochschulen/Notebook_HS.pdf]

3.2 WEP

Funknetze sind offensichtlich leichter abzuhören oder zu beeinflussen als drahtgebundene Netze oder gar Lichtwellenleiter. In Anerkennung dieser Tatsache wurde als Bestandteil von 802.11 eine Technologie unter der Bezeichung **Wired Equivalent Privacy (WEP)** entwickelt.
Diese soll ein Abhören der Funkübertragung verhindern oder zumindest erschweren. Ein sekundäres Ziel war die Realisierung einer Zugriffskontrolle auf das WLAN. WEP soll etwa das Sicherheitsniveau eines Kabel-Ethernet erreichen, die Realisierung hat mehrere Elemente:

- Verschlüsselung mit ***Stream Cipher* RC4**
- den Partnern ist ein geheimer Schlüssel bekannt
- **Integrity Check (IC)** CRC-32 zur Integritätsprüfung
- 24 Bit **Initialization Vector (IV)**

Im Laufe des letzten Jahres sind einige signifikante (und vermeidbare) Schwachstellen von WEP gefunden worden:

- Der IV-Raum ist zu klein; ein IV wiederholt sich nach einigen Stunden, damit liegt dann auch der gleiche Schlüsselstrom vor.
- Wenn **ein** Klartext bekannt ist, dann kann der dazugehörige Schlüsselstrom durch XOR ermittelt werden. Damit sind dann alle verschlüsselten Texte, die den gleichen IV verwenden, entschlüsselbar.
- Die Kenntnis eines Klartexts zu einem verschlüsselten Text ist leichter zu erlangen, als man auf den ersten Blick glaubt. Beispielsweise kann man einen bekannten Klartext von einem beliebigen Host außerhalb des WLAN an eine Mobilstation schicken.

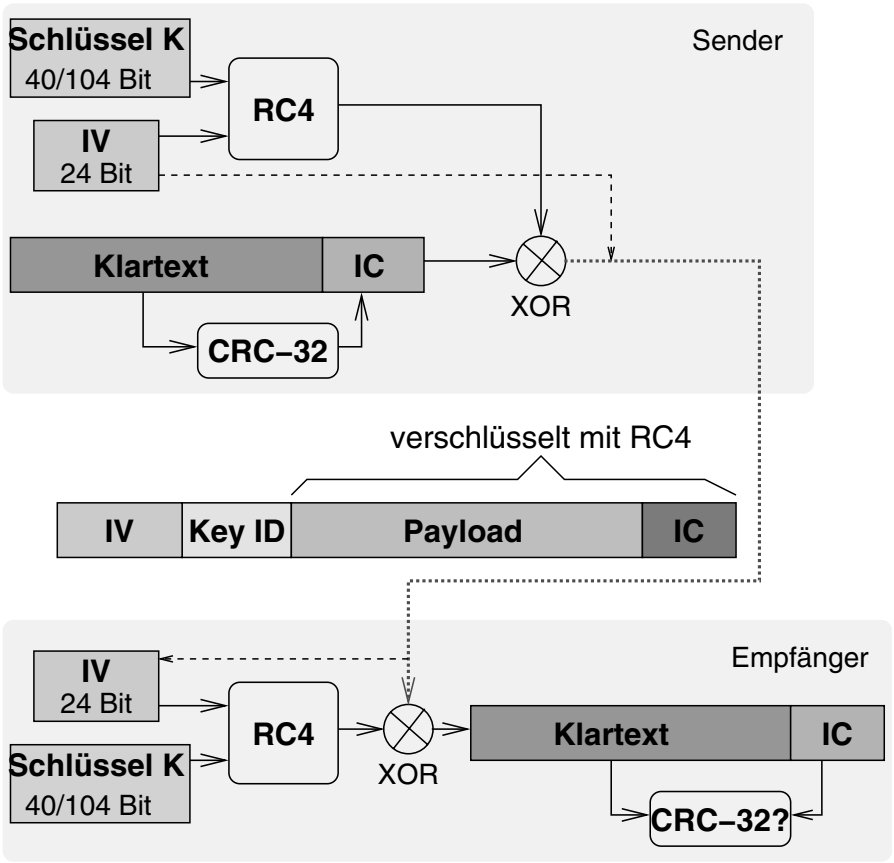

Abbildung 16: WEP-Funktionsweise

- Die Integritätsprüfung mittels CRC-32 kann nur zufällige Fehler mit hoher Wahrscheinlichkeit erkennen. Bei absichtlichen Modifikationen kann auch ohne Kenntnis des Klartext-Inhalts der CRC-32-Wert wieder „passend“ gemacht werden.
  Das läßt sich beispielsweise ausnutzen, um die Ziel-IP-Adresse auf einen beliebigen Host außerhalb des WLAN zu ändern. Der AP entschlüsselt dann den betreffenden Datenstrom.
- Ein Klient weist zur Authentifizierung die Kenntnis des Schlüssels nach:

  *Ein Mithörer kennt jetzt Klartext **und** verschlüsselten Text,*
  er kann daraus den RC4-Strom bestimmen (für einen IV).
  Ein Mithörer kann nun eine andere Challenge korrekt beantworten!
- Die Verteilung der geheimen Schlüssel ist nicht trivial. Allen Nutzern (auch Gästen) muß der geheime Schlüssel bekanntgegeben werden.
  Ein öffentlicher Aushang ist hierzu sicher nicht optimal, etwas besser ist z.B. die Lieferung dieser Information nach Authentifizierung über einen anderen Weg (geschützte

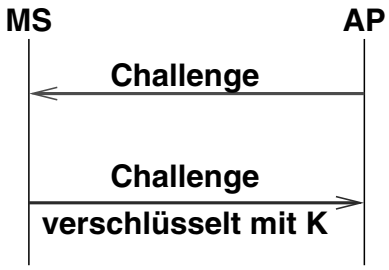

Abbildung 17: WEP-Authentifizierung

WWW-Seite ...).
Eine Alternative wäre das Einsammeln der Laptops und die Schlüsseleinstellung durch eine vertrauenswürdige zentrale Stelle. Beide Verfahrensweisen haben Nachteile. Auch die in den meisten APs gegebene Möglichkeit, eine kleine Anzahl verschiedener Schlüssel einzustellen, mildert das Problem nur wenig.

Aus den geschilderten Schwachstellen sollten Sie folgende Konsequenzen ziehen:

➡ **... kurze Schlüsselnutzungszeiten**

Ein automatisiertes Schlüsselmanagement kann die beschriebenen Schwachstellen teilweise beheben. Einige Produkte enthalten entsprechende Zusätze, die Interoperabilität ist dann aber möglicherweise nicht gegeben.

➡ **... Firewalls/SSH/SSL nutzen**

Beim heutigen Stand der Technik ist die Verwendung von etablierten Techniken in anderen Schichten empfehlenswert.

Literaturhinweis:

Security of the WEP algorithm
[http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html]
Analyse der Schwachstellen

3.3 Authentifizierungsmechanismen

Eine **Authentifizierung** der WLAN-Nutzer brauchen wir aus mehreren Gründen:

- nur festgelegte Nutzer/Nutzerklassen zulassen
- Ressourcenbegrenzung (Bandbreiten/Datenmengen) ?
- Abrechnung (*Accounting*)

Zur Identifikation eines Nutzers gibt es eine ganze Reihe unterschiedlicher Ansätze. Einige sind eher für kleine, selten wechselnde Nutzermengen geeignet; für große Nutzermengen sind nicht alle Verfahren praktikabel.

- Kenntnis des
  Network Name, SSID,
  Extended Service Set IDentifier (ESSID)
  Der Nutzer weist hier nur nach, daß er einen Netzidentifikator kennt. Wenn dies als „Netzpaßwort“ gehandhabt werden soll, ergeben sich dieselben logistischen Hürden wie bei der Verteilung geheimer WEP-Schlüssel.
  Ein offenes Netz akzeptiert Mobilstationen ohne Netzidentifikator. Für die Einschränkung auf Mobilstationen, die den SSID kennen, findet man mitunter die Bezeichnung *„Closed Network“* (das ist wohl etwas irreführend).
- MAC-Adresse - *48 Bit*
  Hier wird im Grunde die WLAN-Karte als „Authentifizierungstoken“ verwendet, was sich ganz gut mit der mancherorts praktizierten Ausleihe von WLAN-Karten organisieren läßt.
  Nachteilig ist der Organisationsaufwand für „fremde“ WLAN-Karten. Außerdem ist eine MAC-Adresse kein Geheimnis, sie läßt sich leicht ermitteln. Weniger bekannt ist die Tatsache, daß sich in vielen Fällen auch beliebige MAC-Adressen einstellen lassen.
- WEP-Authentifizierung - *shared secret key*
  Wie wir im letzten Abschnitt gesehen haben, ist diese Variante eher kontraproduktiv.
- VPN-Authentifizierung (PPTP, IPSec ..)
  Viele VPN-Technologien enthalten Vorkehrungen zur Authentifizierung gegenüber dem anderen Tunnelende, so etwas ist natürlich nutzbar.
  Hier greifen die Eigenschaften (und potentiellen Schwachstellen) der verwendeten VPN-Technologie.
- Nutzername/Paßwort via HTTPS
  Die Nutzer müssen sich über eine Anwendung authentifizieren. Die Authentifizierungsinformationen (z.B. Nutzername und Paßwort) müssen hinreichend sicher übertragen werden, was beispielsweise mit HTTP über SSL/TLS gegeben ist.
  Diese Lösung ist recht einfach durch Nutzer und Management zu handhaben. In Kauf zu nehmen sind die begrenzte Sicherheit der zeitlichen Kontinuität sowie die potentielle Nutzung des WLAN-Segments ohne Authentifizierung.
- *Port-based access control - IEEE802.1x*
  Das ist eine neue Entwicklung zur Authentifizierung von Netzzugängen. Im Fokus befinden sich nicht nur WLAN-Zugänge, sondern z.B. auch Ethernet-Dosen mit mehr oder weniger öffentlichem Zugang.
  Diese Technik ist Teil der neuen IEEE-Sicherheitsarchitektur **Robust Security Network (RSN)**. Es wird das **Extensible Authentication Protocol (EAP)** verwendet, hier konkret **EAP over Wireless (EAPoW)**.

Einige der Verfahren sind kombinierbar, was Schwachstellen kaschieren kann.
Problematisch ist oft die Erkennung der Kontinuität bzw. des Nutzungsendes für einen autorisierten Nutzer.

Für die Verwaltung von Authentifizierungsdaten sollte möglichst auf etablierte und für andere Zwecke oft ohnehin vorhandene Techniken zurückgegriffen werden, wie z.B.

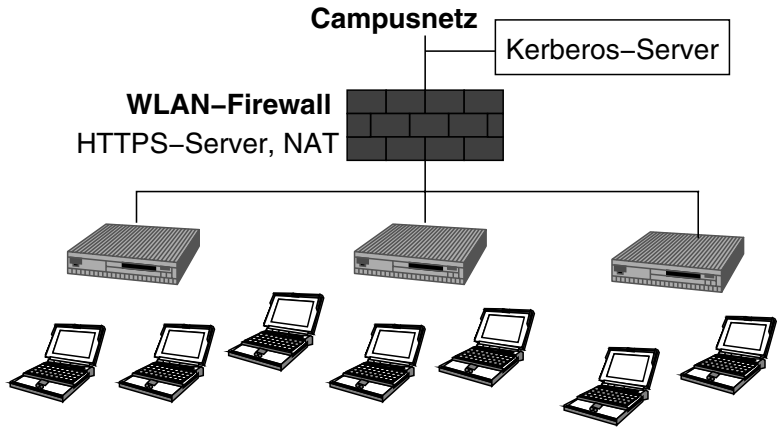

Abbildung 18: WLAN-Authentifizierungsvariante

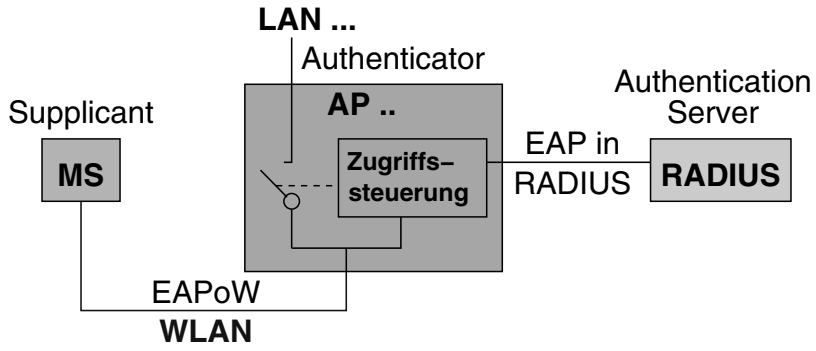

Abbildung 19: EAP-Anwendung bei WLANs

- **Remote Authentication Dial In User Service (RADIUS)**, RFC 2865
- Kerberos
- Directory-Systeme (LDAP ...)

Zum Schluß sei noch auf einen häufiger anzutreffenden Fehler hingewiesen. Ein WLAN-Zugang gehört nicht an die **Innenseite** eines Firewalls, der ein Netz schützt. Der WLAN-Zugang sollte entweder eigene Firewall-Technik erhalten oder einen vorhandenen Firewall so nutzen, daß die WLAN-Nutzer nur die Rechte eines externen Systems haben.

Literaturhinweise:

NoCatNet
[http://nocat.net]
wireless authentication solution, gute Linksammlung

http://www.tu-chemnitz.de/urz/netz/wlan/

mit HTTPS-Authentifizierung

Open1x - Opensource Implementation of IEEE 802.1x
[http://www.open1x.org/]
gute Detailerläuterung zu 802.1x, Hinweis auf Implementierungen

3.4 Vertraulichkeit

Eine mögliche Vorkehrung zur Sicherung der Vertraulichkeit ist die Verwendung der WEP-Verschlüsselung. Trotz der bekannten Schwachstellen ist das sicher besser als gar keine Vorkehrungen. Andererseits wird man bei etwas höheren Anforderungen nicht um zusätzliche oder alternative Techniken herumkommen. Dieser Abschnitt soll primär Lösungen „oberhalb“ von WEP kurz darstellen.

- **Virtual Private Networks (VPN)**
  - **IPSec**
    Bei den ersten Standardentwürfen zu IPSec hatte man übrigens ähnliche Fehler gemacht wie bei WEP. Mittlerweile kann IPSec aber als einigermaßen solide gelten. Als Nachteil bleibt die meist nicht triviale und schwer auf Korrektheit zu prüfende Konfigurierung (vor allem in Endsystemen).
  - **Point-to-Point Tunneling Protocol (PPTP)**
    Diese Variante ist im *Windows*-Umfeld recht verbreitet. Es gibt allerdings auch hier eine Reihe signifikanter und gern ausgenutzter Schwachstellen.
  - **Layer 2 Tunneling Protocol (L2TP)**
    Hinter dieser Variante stehen IETF und große Routerhersteller.
- **End-zu-End-Verschlüsselung und -Authentifizierung**
  - **Secure Sockets Layer (SSL)**
    Transport Layer Security (TLS)
  - **Secure Shell (SSH)**

Literaturhinweise:

Virtual Private Network Consortium
[http://www.vpnc.org/]
IPSec, PPTP ...

OpenSSH
[http://www.openssh.com/]
eine verbreitete SSH-Implementierung

4 Netzstrukturierung und -planung

4.1 Funkausbreitung, Antennen

Bei drahtgebundenen LANs sind gewisse Dimensionierungsvorschriften einzuhalten, z.B. hinsichtlich der Leitungslängen. Drahtlose Netze haben hier weit mehr Variablen, so daß eine Planung anspruchsvoller wird. Für den funktechnischen Teil wird folgender Planungsablauf empfohlen:

1. Voruntersuchung der Ausbreitungsbedingungen und potentieller AP-Standorte
2. Klärung der Infrastruktur-Anbindung der APs
3. Zuordnung der HF-Kanäle zu APs
4. Installation, Verifikationsmessungen

Die **Funkausbreitung** in den hier interessierenden Frequenzbereichen folgt schon weitgehend den Prinzipien der Optik, nach Möglichkeit sollte freie Sicht zwischen Sender und Empfänger bestehen - **Line of Sight (LoS)**.

Bei der Betrachtung der Funkausbreitung werden einige Begriffe und Maße gebraucht:

- dB - logarithmisches Dämpfungs- oder Verstärkungsmaß
- dBi - Antennengewinn gegenüber einem (theoretischen) Isotropstrahler
  2.15 dBi = 0 dB Dipol
- dBm - logarithmisches Leistungsmaß
  `P [dBm] = 10 log P [mW]`
- **Effective Isotropic Radiated Power (EIRP)**
  Eine Bündelung (Antennengewinn) wirkt wie eine Leistungserhöhung:
  $EIRP\ [dBm] = P_S\ [dBm] + G_S\ [dBi]$
- **Ausbreitungsdämpfung (*path loss*)**

Für die Ausbreitungsdämpfung läßt sich diese grobe Abschätzung angeben:

```
L = 20 log(d) + 20 log(f) + 32.44

d - Entfernung [km]
f - Frequenz [MHz]
L - Ausbreitungsdämpfung im Freiraum [dB]
```

Als überschlägige Planungsgrundlage für 802.11b können diese Entfernungsangaben dienen:

```
1     2    5.5    11 Mbit/s
500  350   260   200 m LoS
100   85    70    55 m „Open Office"
45    40    35    30 m „Closed Office"
```

Eine Berücksichtigung der baulichen Besonderheiten ist mit Hilfe einer Ausbreitungs-Vorhersage durch Simulation möglich. Bei der WLAN-Planung werden solche Verfahren aber noch eher selten verwendet, weil die exakte Gebäudegeometrie, Materialien, Materialeigenschaften usw. nur aufwendig zu beschaffen sind. Hier sehen Sie ein Beispiel mit einer punktförmigen Quelle:

Literaturhinweise:

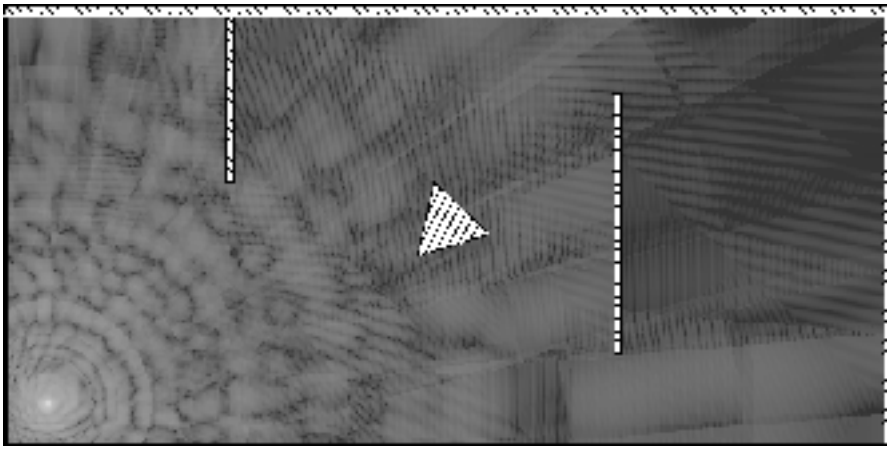

Abbildung 20: Resultat einer Ausbreitungs-Simulation

Low Cost Wireless Network How-To
[http://www.qsl.net/n9zia/wireless/]

zwar speziell für Proxim, auch Abkürzungserläuterungen,Design-Software, umfangreiche Link-Sammlung ...

[http://www.ecommwireless.com/]

einfache Berechnungshilfen

4.2 Produkte und Eigenschaften

Auf dem sehr dynamischen Gebiet WLAN wechselt das Produktspektrum recht häufig (selbst die Herstellernamen bleiben von Änderungen nicht verschont). Wir wollen hier auch kein Marketing für einzelne Produkte machen, sondern einige wesentliche Produktklassen und Unterscheidungsmerkmale anführen:

- **Client Adapter (CA)**
  In manchem neueren mobilen Gerät sind WLAN-Adapter fest eingebaut, hier sind ggf. die Besonderheiten nationaler Zulassungsbedingungen zu beachten (nutzbare Kanäle ...). In den meisten Fällen werden heute austauschbare Adapter eingesetzt, die es für unterschiedliche Schnittstellen und Formfaktoren gibt:
  - PCMCIA/PC-Card (Cardbus)
  - Compact Flash (kleiner als PC-Card, für PDAs)
  - PCI (eher wenig gebräuchlich)
  - USB (die praktikabelste Variante für Desktops)
- **Access Point (AP)**
  Hier gibt es eine größere Anzahl von Unterscheidungsparametern:

- Basis-Funktionalität (L2-Bridge ...)
- Anzahl der Kanäle (typisch 1 .. 2)
- Festnetz-Schnittstelle (typisch 100 BASE TX)
- WEP- und andere Sicherheitsparameter
- Filterfunktionen
- Management-Schnittstellen
- zulässige Umgebungsbedingungen
- Stromversorgung: z.B. **Power over Ethernet (PoE)**

Die PoE-Technologie ist nicht nur für WLAN-APs nützlich, auch IP-Telefone und andere Kleingeräte sind typische „Kunden". Die Einspeisung in das Ethernet-TP-Kabel erfolgt durch einen Ethernet-Switch selbst (noch selten) oder durch einen davor angeordneten **PoE-Injector**. Die technischen Details der einzelnen PoE-Lösungen sind oft noch herstellerspezifisch. Eine Verbesserung dieser unbefriedigenden Situation kann man sich vom Standardentwurf IEEE 802.3af versprechen, der auch Vorkehrungen für Tests und Aushandlung der Stromversorgung vorsieht:

IEEE P802.3af DTE Power via MDI Task Force
[http://grouper.ieee.org/groups/802/3/af/]

– **Residential Gateway**
Das ist ein einfacher AP, der zusätzlich diese Funktionalitäten enthält:
+ Modem/ISDN/DSL-Link
+ **Network Address Translation (NAT)**
+ **Dynamic Host Configuration Protocol (DHCP)**

Hier noch ein Hinweis auf die relevanten Industrie-Konsortien:

Wireless Ethernet Compatibility Alliance (WECA)
[http://www.wi-fi.org/]
– *Wi-Fi steht für 802.11b-Kompatibilität*
– *Wi-Fi5 steht für 802.11a-Kompatibilität (5 mal schneller ;-)*

Wireless Lan Alliance
[http://www.wlana.com/]

5 Ausblicke und Literaturhinweise

Zum Schluß wollen wir uns der Frage zuwenden, ob WLANs die klassischen Ethernet-LANs mit *Twisted Pair* oder Lichtwellenleiter als Medium ablösen werden. Zunächst können wir feststellen, daß das Marktsegment der WLANs momentan offenbar sehr schnell wächst. Dabei gibt es wie eingangs erläutert genügend Anwendungsfälle, in denen WLANs eindeutige Vorteile versprechen.

Eine weitgehende **Ablösung** von Ethernet-LANs in großem Stil ist kurzfristig wenig wahrscheinlich, weil der Bandbreite-Vorsprung der Festnetz-Technologien bei einem Faktor von 10 .. 100 liegt. Bei heutigen Ethernet-LANs liegt die Datenrate eines Einzelanschlusses bei 100 Mbit/s oder 1 GBit/s (in Kürze 10 GBit/s).

Im Vergleich dazu kommt man bei WLANs auf 5 .. 50 Mbit/s, die sich dann oft noch mehrere Stationen teilen.

Es wird eine gegenseitige Ergänzung der Netztechnologien eintreten. Ethernet-LANs können als Backbone des WLANs dienen (und nebenbei auch die Stromversorgung der APs übernehmen).

Die WLAN-Technik selbst entwickelt sich natürlich auch weiter. Zu nennen wären hier erste Produkte, die bei 802.11a mit Kanalbündelung rund 100 Mbit/s erreichen. Bei noch höheren Bandbreiteforderungen orientiert man sich auf bisher noch kaum genutzte Frequenzspektren „oberhalb“ der heutigen.

Die Sicherheitsprobleme werden zunehmend besser verstanden und beherrscht, wobei aber der Prozentsatz der „unsicheren“ WLANs hoch bleiben wird.

Schließlich ist der erwähnte drahtgebundene Backbone keineswegs zwingend. Es gibt zunehmend Versuche, mittels WLAN-Technik auch die Infrastruktur selbst zu realisieren. Dabei sind neben den Bandbreitenproblemen noch eine ganze Anzahl weiterer Herausforderungen (Routing, Management ...) zu meistern. Erste *„Wireless-ISPs“* und *„Wireless Community Networks“* demonstrieren neue Einsatzfelder, teilweise auch neue, unkonventionelle Geschäftsmodelle.

Ausführlichere Informationen und aktualisierte Links zum Thema dieses Tutoriums finden Sie unter:

http://rnvs.informatik.tu-chemnitz.de/wlan/

Weitere Literaturhinweise/Portale:

O’Reilly Network: Wireless DevCenter
[http://www.oreillynet.com/wireless]

802.11b/WiFi News
[http://80211b.weblogger.com/]

Rob Flickenger: Building Wireless Community Networks.
O’Reilly, 2001, ISBN 0-596-00204-1, 138 S.
http://www.oreilly.com/catalog/wirelesscommnet/